Community Bankers of Michigan Regulatory Dispatch

March 22, 2022

Timely news and resources community bankers can use

to better stay on top of a rapidly changing world.

CFPB Targets Unfair Discrimination in Consumer Finance

WASHINGTON, D.C. — The Consumer Financial Protection Bureau (CFPB) announced changes to its supervisory operations to better protect families and communities from illegal discrimination, including in situations where fair lending laws may not apply. In the course of examining banks and other companies' compliance with consumer protection rules, the CFPB will scrutinize discriminatory conduct that violates the federal prohibition against unfair practices. The CFPB will closely examine financial institutions' decision-making in advertising, pricing, and other areas to ensure that companies are appropriately testing for and eliminating illegal discrimination.

"When a person is denied access to a bank account because of their religion or race, this is unambiguously unfair," said CFPB Director Rohit Chopra. "We will be expanding our anti-discrimination efforts to combat discriminatory practices across the board in consumer finance."

The CFPB enforces several laws that can target discriminatory practices. Government regulators and private plaintiffs have commonly relied on the Equal Credit Opportunity Act (ECOA), a fair lending law which covers extensions of credit. However, certain discriminatory practices may also trigger liability under the Consumer Financial Protection Act (CFPA), which prohibits unfair, deceptive, and abusive acts and practices (UDAAPs).

The CFPB published an updated exam manual today for evaluating UDAAPs, which notes that discrimination may meet the criteria for "unfairness" by causing substantial harm to consumers that they cannot reasonably avoid, where that harm is not outweighed by countervailing benefits to consumers or competition. Consumers can be harmed by discrimination regardless of whether it is intentional. Discrimination can be unfair in cases where the conduct may also be covered by ECOA, as well as in instances where ECOA does not apply. For example, denying access to a checking account because the individual is of a particular race could be an unfair practice even in those instances where ECOA may not apply.

The CFPB will examine for discrimination in all consumer finance markets, including credit, servicing, collections, consumer reporting, payments, remittances, and deposits. CFPB examiners will require supervised companies to show their processes for assessing risks and discriminatory outcomes, including documentation of customer demographics and the impact of products and fees on different demographic groups. The CFPB will look at how companies test and monitor their decision-making processes for unfair discrimination, as well as discrimination under ECOA.

Comment: In the press release, the CFPB suggests that it will use the Unfair, Deceptive, and Abusive Acts and Practices (UDAAP) doctrine to target what they are calling 'unintentional' discriminatory practices and practices that fall outside of traditional 'fair lending' concerns found in the Equal Credit Opportunity Act. For example, "denying access to a checking account because the individual is of a particular race could be an unfair practice even in those instances where ECOA may not apply." This UDAAP approach to 'unintentional discrimination' represents a substantial expansion of the CFPB's authority to police practices the CFPB deems discriminatory or 'unfair.' Obviously, there would be concern if a bank refused to open accounts for a particular protected class. The trickier compliance issue is whether a bank's marketing campaigns are able to withstand scrutiny. Although few community banks are directly examined by the CFPB, we can expect the other federal regulators to follow suit.

Items of Interest

Bank Management

	FRB Industrial Production and Capacity Utilization - G.17 (03.17.2022) - Total industrial production rose 0.5 percent in February to a level that is 103.6 percent of its 2017 average. Manufacturing output increased 1.2 percent after having been little changed in each of the previous two months. In February, the index for utilities declined 2.7 percent, and the output of mines edged up 0.l percent. Total industrial production in February was 7.5 percent higher than its year-earlier level, but severe winter weather in February 2021 significantly suppressed industrial activity that month. A more useful comparison shows that the index has advanced a still-strong 4.2 percent since January 2021. Capacity utilization for the industrial sector increased 0.3 percentage point in February to 77.6 percent, a rate that is 1.9 percentage points below its long-run (1972–2021) average.
	FRB FOMC Statement (03.16.2022) - Indicators of economic activity and employment have continued to strengthen. Job gains have been strong in recent months, and the unemployment rate has declined substantially. Inflation remains elevated, reflecting supply and demand imbalances related to the pandemic, higher energy prices, and broader price pressures. The invasion of Ukraine by Russia is causing tremendous human and economic hardship. The implications for the U.S. economy are highly uncertain, but in the near term the invasion and related events are likely to create additional upward pressure on inflation and weigh on economic activity. The Committee seeks to achieve maximum employment and inflation at the rate of 2 percent over the longer run. With appropriate firming in the stance of monetary policy, the

	Committee expects inflation to return to its 2 percent objective and the labor market to remain strong. In support of these goals, the Committee decided to raise the target range for the federal funds rate to 1/4 to 1/2 percent and anticipates that ongoing increases in the target range will be appropriate. In addition, the Committee expects to begin reducing its holdings of Treasury securities and agency debt and agency mortgage-backed securities at a coming meeting. In assessing the appropriate stance of monetary policy, the Committee will continue to monitor the implications of incoming information for the economic outlook. The Committee would be prepared to adjust the stance of monetary policy as appropriate if risks emerge that could impede the attainment of the Committee's goals. The Committee's assessments will take into account a wide range of information, including readings on public health, labor market conditions, inflation pressures and inflation expectations, and financial and international developments. Voting for the monetary policy action were Jerome H. Powell, Chair; John C. Williams, Vice Chair; Michelle W. Bowman; Lael Brainard; Esther L. George; Patrick Harker; Loretta J. Mester; and Christopher J. Waller. Voting against this action was James Bullard, who preferred at this meeting to raise the target range for the federal funds rate by 0.5 percentage point to 1/2 to 3/4 percent. Patrick Harker voted as an alternate member at this meeting. ***Comment: The following is a statement by Federal Reserve Bank of St. Louis President Jim Bullard explaining his dissenting vote at the FOMC's March 15-16, 2022, meeting:*** ***"I dissented with the Federal Open Market Committee (FOMC) decision announced on March 16, 2022, to raise the target range for the federal funds rate by 25 basis points to 0.25% to 0.50%. In my view, raising the target range to 0.50% to 0.75% and implementing a plan for reducing the size of the Fed's balance sheet would have been more appropriate actions." Read more of Bullard's comments here.***
	CSBS Blog 7 of 7: Community Bankers' View of Technology (03.15.2022) - By CSBS Chief Economist Thomas F. Siems, Temple University Professor of Finance and CSBS Adjunct Research Scholar Jonathan A. Scott and Federal Reserve Bank of St. Louis Supervision Policy, Research and Analysis Manager Meredith A. Covington. **ADAPTING TO THE DIGITAL AGE SERIES** • Blog 1: Macroeconomic Forces • Blog 2: Competitive Forces • Blog 3: Tech Usage (log in required to view this blog) • Blog 4: Is Tech an Opportunity or a Threat? • Blog 5: How are Core Services Providers Viewed? • Blog 6: Tech Investment and Mergers and Acquisitions • Blog 7: Community Bankers' View of Technology In this seven-part blog series, we explore how community banks are adapting to a changing digital landscape by analyzing banking and technology questions from the 2021 CSBS National Survey of Community Banks. Survey results are presented each fall at the

	annual Community Banking in the 21st Century Research and Policy Conference, sponsored by CSBS, the Federal Reserve and the Federal Deposit Insurance Corp. In the seventh installment in this series, we share interview responses with community bankers from around the nation on their views about technology.
	FDIC Rescission of Statement on Part 363 Annual Reports in Response to the Coronavirus (03.15.2022) - On March 27, 2020, the FDIC issued Financial Institution Letter (FIL-30-2020), Statement on Part 363 Annual Reports in Response to the Coronavirus, which provided an additional 45 days for insured depository institutions (IDIs) subject to Part 363 of the FDIC's regulations to file their Part 363 Annual Reports and Other Reports and Notices. The FDIC, in consultation with federal and state financial regulators, is rescinding FIL-30-2020. Statement of Applicability: This Financial Institution Letter applies to all insured depository institutions with $500 million or more in total assets. Highlights: The FDIC rescinds FIL-30-2020, which provided a 45-day extension of time for filing Part 363 Annual Reports. • The rescission is effective for fiscal years beginning after December 31, 2021. The deadline for filing the annual report for fiscal years beginning after December 31, 2021 reverts to either 90 or 120 days after the end of the IDI's fiscal year, depending on the IDI's status as a public filer. • IDIs are reminded that the provisions of §363.4(e) and Guideline 23 to Part 363 regarding the Notification of Late Filing remain applicable for fiscal years beginning after December 31, 2021. Thus, to the extent that an IDI is unable to timely file all or any portion of its annual report, the IDI must submit a written Notice of Late Filing to the FDIC, the appropriate federal banking agency, and any appropriate state bank supervisor by the 90- or 120-day report filing deadline. These provisions also apply to any IDI subject to Part 363 of the FDIC's regulations that may be unable to submit its Part 363 Annual Report in a timely manner due to the effects of the pandemic. • The FDIC affirms that the staff of the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the state banking regulators have acknowledged the FDIC's treatment of the annual report required by Part 363. ***Comment: If your bank falls within the requirements of this section, be sure to update procedures to timely file your 363 Annual Report.***

BSA / AML

	FinCEN Announces $140 Million Civil Money Penalty against USAA Federal Savings Bank for Violations of the Bank Secrecy Act (03.17.2022) - WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) today announced that it has assessed a $140 million civil money penalty against USAA Federal Savings Bank (USAA FSB) for willful violations of the Bank Secrecy Act (BSA) and its implementing regulations. Specifically, USAA FSB admitted that it willfully failed to implement and maintain an anti-money laundering (AML) program that met the minimum requirements of the BSA from at least January 2016 through April 2021. USAA FSB also admitted that it willfully failed to accurately and timely report thousands of suspicious transactions to FinCEN involving suspicious financial activity by its customers, including customers using personal accounts for apparent criminal activity. "As its customer base and revenue grew in recent years, USAA FSB willfully failed to ensure that its compliance program kept pace, resulting in millions of dollars in suspicious transactions flowing through the U.S. financial system without appropriate reporting," said FinCEN's Acting Director Himamauli Das. "USAA FSB also received ample notice and opportunity to remediate its inadequate AML program, but repeatedly failed to do so. Today's action signals that growth and compliance must be paired, and AML program deficiencies, especially deficiencies identified by federal regulators, must be promptly and effectively addressed." The Office of the Comptroller of the Currency (OCC) assessed a civil penalty of $60 million for related violations. As many of the facts and circumstances underlying the OCC's civil penalty also form the basis of FinCEN's Consent Order, FinCEN agreed to credit the $60 million civil penalty imposed by the OCC. Taken together, USAA FSB will pay a total of $140 million to the U.S. Treasury for its violations, with $80 million representing FinCEN's penalty and $60 million representing the OCC's penalty. FinCEN's Office of Enforcement is responsible for investigating serious violations of the BSA. For additional information regarding the facts and circumstances associated with this enforcement action, including the specific BSA violations and their underlying causes, please see the Consent Order between FinCEN and USAA FSB here. ***Comment: Usually in these sorts of situations, the bank 'admits to no wrongdoing' but not in this case. Seldom do we see words like 'willful' and 'admitted' in the same sentence.***
	OCC Issues Final Rule Addressing Authority for Exemptions to Suspicious Activity Report Requirements (03.16.2022) - WASHINGTON—The Office of the Comptroller of the Currency (OCC) issued a final rule amending the OCC's suspicious activity report (SAR) regulations. The rule clarifies the OCC's authority to issue exemptions from the requirements of those regulations based on a request from a national bank or federal savings association, including federal branches and agencies of foreign banks. The rule provides that, for any

	SAR regulation exemption request, the OCC will consider criteria specified in the final rule, including consistency with the purposes of the Bank Secrecy Act and safe and sound banking. The final rule adopts, with changes in response to public comments, the proposed rule published in the Federal Register on January 22, 2021. The final rule takes effect on May 1, 2022. For exemption requests from the OCC's SAR regulation that also would require an exemption from the SAR requirements established by the Financial Crimes Enforcement Network (FinCEN), a national bank or federal savings association would need to seek an exemption from both the OCC and FinCEN. The OCC intends to coordinate with FinCEN on any such request. Related Link Federal Register Notice (PDF) ***Comment: The process to request an exemption is amazingly vague. No time frames are spelled out. Also, be sure that any exemption is also approved by FinCEN.***

Deposit / Retail Operations

	No news to report this week.

Human Resources

	No news to report this week.

Lending

	No news to report this week.

Technology / Security

	CISA Mitigating Threats Posed By Russian State-Sponsored Cyber Actors' Exploitation of Default Multifactor Authentication Protocol and "Printnightmare" Vulnerability (03.15.2022) - WASHINGTON – The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) issued a joint cybersecurity advisory with technical details, mitigations, and resources regarding previously demonstrated ability of Russian state-sponsored cyber actors to gain network access through exploitation of default multifactor authentication (MFA) protocols and a known vulnerability in Windows Print Spooler, "PrintNightmare." As early as May 2021, the Russian state-sponsored cyber actors took advantage of a misconfigured account set to default MFA protocols at a non-governmental organization, allowing them to enroll a new device for MFA and access the victim's network. The actors then exploited a critical vulnerability "PrintNightmare" (CVE-2021-34527) to run arbitrary

code with system privileges, and then were able to access cloud and email accounts for document exfiltration.

This advisory, titled "Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and 'PrintNightmare' Vulnerability," provides observed tactics, techniques, and procedures (TTPs); indicators of compromise (IOCs); and mitigation recommendations. The FBI and CISA urge all organizations to take immediate action to protect against this malicious activity and apply recommended mitigations such as:

- Enforce MFA for all users, without exception, and ensure it is properly configured to protect against "fail open" and re-enrollment scenarios
- Implement time-out and lock-out features
- Disable inactive accounts uniformly in active directory, MFA, etc.
- Update software, prioritizing known exploited vulnerabilities
- Monitor network logs continuously for suspicious activity
- Implement security alerting policies

"At CISA, we are great believers in multifactor authentication. It remains one of the most effective measures individuals and organizations can take to reduce their risk to malicious cyber activity. This advisory demonstrates the imperative that organizations configure MFA properly to maximize effectiveness," said CISA Director Jen Easterly. "Now, more than ever, organizations must put their shields up to protect against cyber intrusions, which means applying the mitigations in this advisory including enforcing MFA for all users without exception, patching known exploited vulnerabilities, and ensuring MFA is implemented securely."

"The FBI, alongside our federal and international partners, will continue to pursue cyber actors who engage in this type of targeted malicious activity of unauthorized access and exfiltration of data," said FBI Cyber Division Assistant Director Bryan Vorndran. "We encourage organizations who may have experienced this type of exploitation to report to the FBI and/or CISA and provide us with additional information so we can continue to deter and disrupt nation-state actors. The FBI will not tolerate this type of criminal activity and we will use all of the tools in our toolbelt to combat this threat."

CISA has updated the Shields Up webpage to include new services and resources, recommendations for corporate leaders and chief executive officers, and actions to protect critical assets. Additionally, CISA has created a new Shields Up Technical Guidance webpage that details other malicious cyber activity affecting Ukraine. The webpage includes technical resources from partners to assist organizations against these threats.

To report a cyber incident, organizations should contact CISA at report@cisa.gov or call CISA's 24/7 CISA Central Operations Center at (888) 282-0870 and/or to the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.

Selected federal rules – proposed

Proposed rules are included only when community banks may want to comment. Date posted may not be the same as the Federal Register Date.

PROPOSED RULE WITH REQUEST FOR PUBLIC COMMENT

01.26.2022 Request for Information Regarding Fees Imposed by Providers of Consumer Financial Products or Services - The Consumer Financial Protection Bureau (Bureau or CFPB) is seeking comments from the public related to fees that are not subject to competitive processes that ensure fair pricing. The submissions to this request for information will serve to assist the CFPB and policymakers in exercising its enforcement, supervision, regulatory, and other authorities to create fairer, more transparent, and competitive consumer financial markets. **DATES: Comments must be received on or before March 31, 2022.**

01.25.2022 Pilot Program on Sharing of Suspicious Activity Reports and Related Information With Foreign Branches, Subsidiaries, and Affiliates - FinCEN is issuing this notice of proposed rulemaking to seek public comment on the proposed establishment of a limited-duration pilot program, subject to conditions set by FinCEN, to permit a financial institution with a suspicious activity report (SAR) reporting obligation to share SARs and information related to SARs with the institution's foreign branches, subsidiaries, and affiliates for the purpose of combating illicit finance risk, in accordance with Section 6212(a) of the Anti-Money Laundering Act of 2020 (AML Act). **DATES: Written comments on this proposed rule must be received on or before March 28, 2022.**